

UTILITY PATENT APPLICATION TRANSMITTAL

☐ DUPLICATE

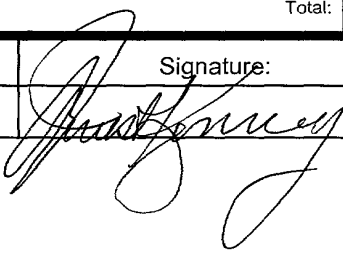
Address to: Commissioner for Patents Box PATENT APPLICATION Washington, DC 20231	Attorney Docket No.	JEK/Grassl
	First Named Inventor (or identifier)	Thomas GRASSL et al.
	Total Pages	

Transmitted herewith is a patent application under 37 CFR 1.53(b).

Entitled: **METHOD FOR PROTECTING A DATA MEMORY**

- ☐ 1. Submitted herewith are the following:
- 8 pages of specification.
 - ☒ Abstract.
 - 2 sheet(s) of drawings.
 - 18 claim(s).
 - ☒ Oath/Declaration unsigned by each inventor.
 - ☐ signed Inventor Small Entity Statement(s).
 - ☐ signed non-Inventor Small Entity Statement(s).
 - ☐ signed Small Business Small Entity Statement(s).
 - ☐ signed Non-Profit Small Entity Statement(s).
 - ☒ Preliminary Amendment.
 - ☐ Information Disclosure Statement(s).
 - ☐ pages of Form PTO-1449, and one copy of each document listed thereon.
 - ☐ Assignment of the invention, Cover Sheet, and payment of the \$_____ recordal fee.
 - ☐ certified copy of application no. _____ filed in _____. Priority is claimed.
 - ☒ check in the amount of \$ 690.00 to cover the filing fee.
- ☒ 2. The Commissioner is authorized to credit any overpayment and charge any deficiency in any fees required under 37 CFR 1.16 and/or 1.17, to Deposit Account No. 02-0200.
- ☐ 3. Insert before the first sentence of the specification: - - This application claims the benefit of provisional application number _____ filed _____. - -
- ☐ 4. Insert before the first sentence of the specification: - - This application is a Continuation-in-part of nonprovisional application number _____ filed _____. - -
- ☐ 5. Other: _____

1c564 U.S. PTO
09/671731
09/29/00

THE FILING FEE IS CALCULATED AS FOLLOWS:				Basic Fee:	\$690.00
Total Claims:	17	- 20 =	0	X \$18 =	0
Independent Claims:	2	- 3 =	0	X \$78 =	0
Correspondence Address: BACON & THOMAS, PLLC 625 Slaters Lane, 4 th Floor Alexandria, VA 22314-1176				Multiple Dependent Claim (add \$260.00)	
				Subtotal:	
				50% Reduction if Small Entity Status:	
Phone: 703-683-0500		Fax: 703-683-1080		Total:	\$690.00
Date:	Name:			Signature:	Reg. No.
September 1, 2000	J. Ernest Kenney				19,179

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Inventor: Thomas GRASSL et al. Examiner: To Be Assigned

Serial No: To Be Assigned Art Unit: To Be Assigned

Filed: September 29, 2000 Atty Dkt: JEK/GRASSL

For: METHOD FOR PROTECTING A DATA MEMORY

PRELIMINARY AMENDMENT

Commissioner of Patents
Washington, D.C. 20231

Sir:

Prior to issuance of an Official Action on the merits, please amend the application as follows.

IN THE CLAIMS:

Please amend the claims as follows.

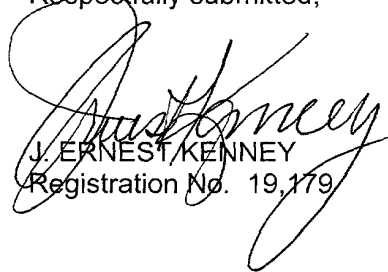
- Claim 3, line 1, delete "or 2".
- Claim 4, line 1, delete "any of claims 1 to 3" and insert -- claim 1 --.
- Claim 7, line 1, delete "any of the above claims" and insert -- claim 1 --.
- Claim 8, line 1, delete "any of claims 5 to 7" and insert -- claim 5 --.
- Claim 9, line 1, delete "any of the above claims" and insert -- claim 1 --.
- Claim 12, line 1, delete "or 11".
- Claim 13, line 1, delete "any of claims 10 to 12" and insert -- claim 10 --.
- Claim 15, line 1, delete "or 14".
- Claim 16, line 1, delete "any of the above claims" and insert -- claim 1 --.

Application No: To Be Assigned
Group Art Unit: To Be Assigned
Examiner: To Be Assigned

[18] (Amended) 17. A smart card terminal having a security processor according to [any of claims 10 to 17] claim 10.

If any issues remain that may be resolved by a telephone or facsimile communication with the Applicant's Attorney, the Examiner is invited to contact the undersigned at the numbers shown below.

Respectfully submitted,



J. ERNEST KENNEY
Registration No. 19,179

BACON & THOMAS, PLLC
625 Slaters Lane - 4th Floor
Alexandria, VA 22314-1176
Telephone: (703) 683-0500
Facsimile: (703) 683-1080

Date: September 29, 2000

S:\Producer\jek\GRASSL - bo DE199475741\Preliminary Amendment frm

Method for protecting a data memory

The present invention relates to a method for protecting a security data memory and a security processor having such a security data memory. The term "security data memory" refers here to any data memory containing security-relevant data which must be protected from unauthorized access.

Such security processors having security data memories are found in particular in smart cards and smart card terminals used to make a data link with a smart card. Since the security-relevant data are stored on the smart cards in coded form, the security processor must be in possession of the right keys to be able to process the smart card data. Said keys are stored in a security data memory. In order to prevent unauthorized persons from acquiring said key data and committing abuse with them, special measures are necessary.

The applicant's EFTPOS terminal is already known from practice. With this terminal the total security module with the security processor including display, keyboard and measuring heads is cast as one unit. A light sensor is located within the casting compound. As soon as said light sensor detects incidence of light, the security processor automatically erases the security-relevant data stored in the security data memory. Unauthorized access from outside would make the terminal inoperable, but a readout of the security-relevant data would no longer be possible.

EP 0 408 456 B2 describes a smart card whose microcircuit is protected from access by a plurality of sensors having a so-called state of prestress. Said sensors react to mechanical deformations. A plurality of sensors are distributed within the smart card in order to monitor the total smart card for attacks.

Said known security measures are reliable, but it is hitherto not possible to obtain information on how an attack was performed after a sensor responds, i.e. after an attack has occurred.

The problem of the present invention is to state a method for protecting a security data memory or a security processor having a security data memory which permits information to be gained on the nature and place of an attack after one has occurred.

This problem is solved by a method according to claim 1 and by a security processor according to claim 10.

The permanent monitoring of the sensors, with the status data of the sensors constantly being stored, permits a log to be recorded indicating after an attack how the statuses of the individual sensors changed before the signaled attack.

The sensors can be any sensors which register different parameters such as temperature, pressure, light, radioactivity, x-rays, electron beams or the like at a great variety of places. This log permits information to be gained on the manner and the spatial area in which an attack was performed. Said data can firstly help to clarify the cause of the attack. Secondly, they can be useful in developing security technology.

The status data of the sensors are preferably stored cyclically in an overwriteable memory by the data recording device, that is, only a certain number of past data records is stored in each case.

In principle the status data can be stored directly in a nonvolatile memory. The status data can also fundamentally be stored in a volatile memory whose permanent power supply is secured in every situation.

Preferably, the cyclic storage of the status data is first effected in a volatile temporary memory and the data are then transferred from the temporary memory to a nonvolatile final memory when an attack is signaled. Additionally, the status data of the sensors, or at least of the one sensor signaling the attack, are advantageously stored directly in the final memory when an attack is signaled.

In an especially time-economic embodiment with a low storage requirement at the same time, the status data of the sensors are passed on for permanent logging to an analog-to-digital converter which digitally codes the analog status data for storage in the volatile temporary memory. Only when an attack is signaled are the status data of the sensors, or the sensor which signaled the attack, stored directly in the final memory without previously running through the analog-to-digital converter and temporary memory.

Since one must expect an attack to be performed only after an interruption in the supply voltage, the security processor is provided with a battery buffer. A battery of course also includes an rechargeable accumulator in this context. This battery

maintains the power supply to the sensors or the security data memory or the other components required for carrying out the method, for example the sensor evaluation device and data recording device, at least until the security-relevant data in the security memory are erased and the recording of the sensor data or transfer of the sensor data from the temporary memory to the final memory is concluded.

In order to ensure that at least the most important and most critical functions are performed even when the intended method cannot be performed completely due to the lack of supply voltage and deficient battery voltage, the following order is observed after an attack has occurred.

First, the security-relevant data in the security memory are erased. In a second step the current status data, at least of the sensor which signaled the attack, are then stored directly in the final memory. Subsequently the status data contained in the temporary memory are transferred to the final memory. When the status data are transferred from the temporary memory to the final memory a backward chronological order is observed, i.e. the most recent status data are transferred to the final memory first and the oldest status data at the end so that the log is as up-to-date as possible.

As described above, such security processors are used mainly within smart card terminals. However, the invention is obviously not restricted to this area of application. The inventive method or a corresponding security processor can be used wherever security-relevant data are to be protected from unauthorized access.

The invention will be explained in more detail in the following by an example with reference to the enclosed drawings. The features shown therein may be essential to the invention not only in the stated combinations but also singly or in other combinations.

Fig. 1 shows a schematic block diagram of the functional arrangement of the sensor evaluation device and data recording device within the security processor,

Fig. 2 shows a schematic block diagram of the sensor evaluation device and data recording device.

The inventive security processor shown in the figures has a plurality of security sensors 2. Various sensors 2 are shown in Fig. 1 as a common block. They may in-

volve a great variety of sensor types, for example light sensors, thermal sensors or sensors reacting to mechanical deformations or vibrations.

The signals of sensors 2 are passed on unchanged, that is, in analog form, via lines 9 to data recording device 6, on the one hand, and via branch 10 to sensor evaluation device 5, on the other hand.

Data recording device or circuit 6 has, at one input to which the analog sensor signals are transmitted via line 9, analog-to-digital converter 7 for digitizing the sensor signals. Said digital sensor signals are then passed on to rewritable, volatile temporary memory 3 and stored there cyclically. That is, the first sensor data record is stored first, then the second sensor data record, etc., until temporary memory 3 is completely occupied with n sensor data records. With the $n+1$ data record the oldest data record, that is, sensor data record 1, is then overwritten. In this way the last n data records are always stored so that a log for a certain, past time period is available at every point in time.

At the same time the sensor signals are evaluated within sensor evaluation device or circuit 5 as to whether one of the sensor signals undershoots or overshoots a given threshold. The thresholds can be freely adjusted for individual sensors 2 in order to vary the sensitivity of the total security circuit.

If the overshoot or undershoot of a threshold is signaled this is regarded as an attack on the security processor. In this case sensor evaluation device 5 actively erases the relevant area in security memory 1 via reset line 13. At the same time a stop command is given to analog-to-digital converter 7 and temporary memory 3 via line 12 for stopping further digitization of the sensor signals and their storage in the temporary memory. Furthermore the sensor signals are passed on via line 11 to data recording device 6 and written there directly to nonvolatile final memory 4 as sensor switching data (Fig. 2).

Subsequently the content of temporary memory 3 is mirrored, i.e. copied, automatically to nonvolatile final memory 4 within data recording device 6. This copy process is performed backwards in time in terms of the age of the data records. That is, the last byte is first recorded from all sensors 2, then the next-to-last byte, etc. The data of the sensor which signaled the attack are transferred first.

When the security processor is started up again after an attack, the CPU of the security processor can then read out final memory 4 via the internal bus and thus filter out the desired information.

Before the next usage, i.e. the refocusing of sensors 2, final memory 4 is erased again after readout so that it only contains the current sensor statuses in the case of a new attack.

In order to ensure the run of the security functions in the case of an attack with the supply voltage interrupted, the security processor is supplied with battery voltage *VBAT* besides supply voltage *VCC*. For this purpose, both supply voltage *VCC* and battery voltage *VBAT* are applied to voltage selection device or circuit 8 of the security processor. Voltage selection device 8 constantly monitors supply voltage *VCC* and ensures that if supply voltage *VCC* drops below a minimal value the decisive components are automatically supplied further with battery voltage *VBAT*. Sensors 2 can in part also be supplied directly with battery voltage *VBAT* permanently.

The abovementioned special order of the individual functional steps ensures that even if battery voltage *VBAT* fails, i.e. if battery voltage *VBAT* drops below a minimal value, most probably at least the erasure of the security-relevant data is guaranteed and furthermore the information is retained preferably in accordance with its importance for later evaluation.

Patent claims

1. A method for protecting a security data memory (1) wherein external action on a component containing the security data memory (1) is detected by sensors (2), an attack being signaled by undershooting or overshooting of a threshold on one of the sensors (2), by reason of which the content of the security data memory (1) is at least partly erased, characterized in that the status of the sensors (2) is permanently monitored and the status data of the sensors (2) recorded.

2. A method according to claim 1, characterized in that the status data of the sensors (2) are stored cyclically in an overwritable memory (3).

3. A method according to claim 1 or 2, characterized in that the status data of the sensors (2) are stored in a nonvolatile memory (4).

4. A method according to any of claims 1 to 3, characterized in that the status data of the sensors (2) are stored in a volatile temporary memory (3) and when an attack is signaled the status data contained in the temporary memory (3) are transferred to a nonvolatile final memory (4).

5. A method according to claim 4, characterized in that when an attack is signaled at least the status data of the sensor signaling the attack are stored directly in the final memory (4).

6. A method according to claim 5, characterized in that the status data are stored in the temporary memory (3) in digitally coded form, and direct storage of the status data in the final memory (4) is done in analog form when an attack is signaled.

7. A method according to any of the above claims, characterized in that if the supply voltage (*VCC*) fails, the power supply to the sensors (2) and/or the security data memory (1) and/or further components (3, 4, 5, 6, 7) required for carrying out the method is maintained with a battery for a certain time period.

8. A method according to any of claims 5 to 7, characterized in that after an attack is signaled the content of the security data memory (1) is first erased, then the current status data at least of the sensor signaling the attack are stored in the final memory (4), and subsequently the status data contained in the temporary memory (3) are transferred to the final memory (4).

9. A method according to any of the above claims, characterized in that the status data stored in the temporary memory (3) are transferred to the final memory (4) in reverse chronological order in terms of their age, the status data of the sensor signaling the attack being transferred first and then the status data of the other sensors.

10. A security processor having a security data memory (1) and sensors (2) for detecting external action on the security processor and/or the security data memory (1), and a sensor evaluation device (5) which at least partly erases the content of the security data memory (1) when a threshold is overshot on one of the sensors (2), characterized by a data recording device (6) which permanently records the status data of the sensors (2) in a memory (3).

11. A security processor according to claim 10, characterized by an overwriteable memory (3) in which the status data of the sensors (2) can be cyclically stored by the data recording device (6).

12. A security processor according to claim 10 or 11, characterized by a non-volatile memory (4) for the status data.

13. A security processor according to any of claims 10 to 12, characterized by a volatile temporary memory (3) in which the status data of the sensors (2) are stored permanently, and a nonvolatile final memory (4) to which the status data contained in the temporary memory (3) are transferred when an attack is signaled.

14. A security processor according to claim 14, characterized by an analog-to-digital converter (7) which digitally codes the analog status data before storage.

15. A security processor according to claim 13 or 14, characterized in that the sensor evaluation device (5) is connected with the final memory (4) and when an attack is signaled at least the status data of the sensor signaling the attack are stored directly in the final memory (4).

16. A security processor according to any of the above claims, characterized by a battery which maintains the power supply to the sensors (2) and/or security data memory (1) and/or sensor evaluation device (5) and/or data recording device (6) and/or memories (3, 4) for the status data of the sensors (2) for a certain time period if the supply voltage (V_{CC}) fails.

18. A smart card terminal having a security processor according to any of claims 10 to 17.

Abstract

A method for protecting a security data memory is described wherein external action on a component containing the security data memory is detected by sensors. Overshooting of a threshold on one of the sensors causes an attack to be signaled by reason of which the content of the security data memory is at least partly erased. The status of the sensors is permanently monitored and the status data of the sensors recorded.

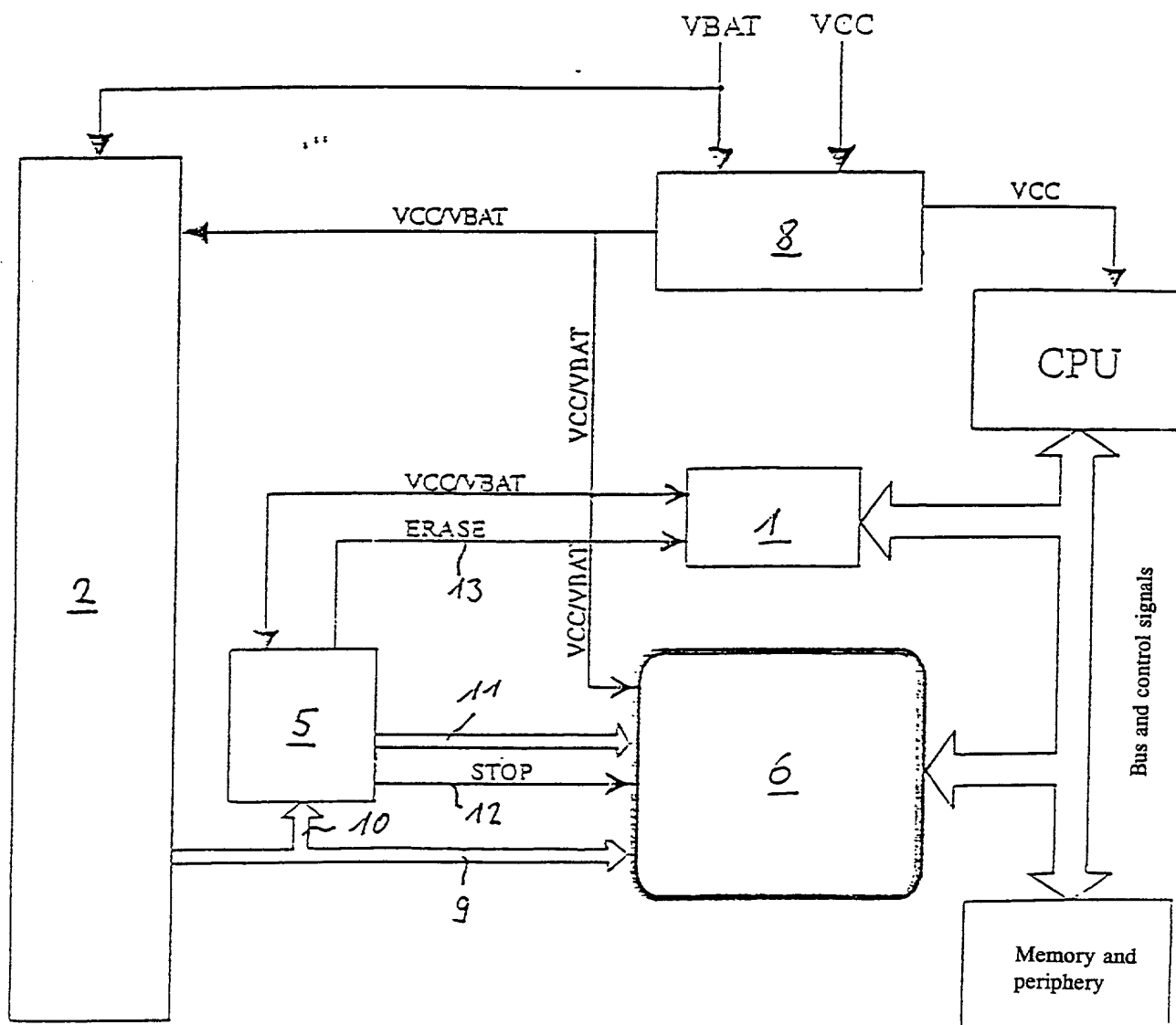


Fig. 1

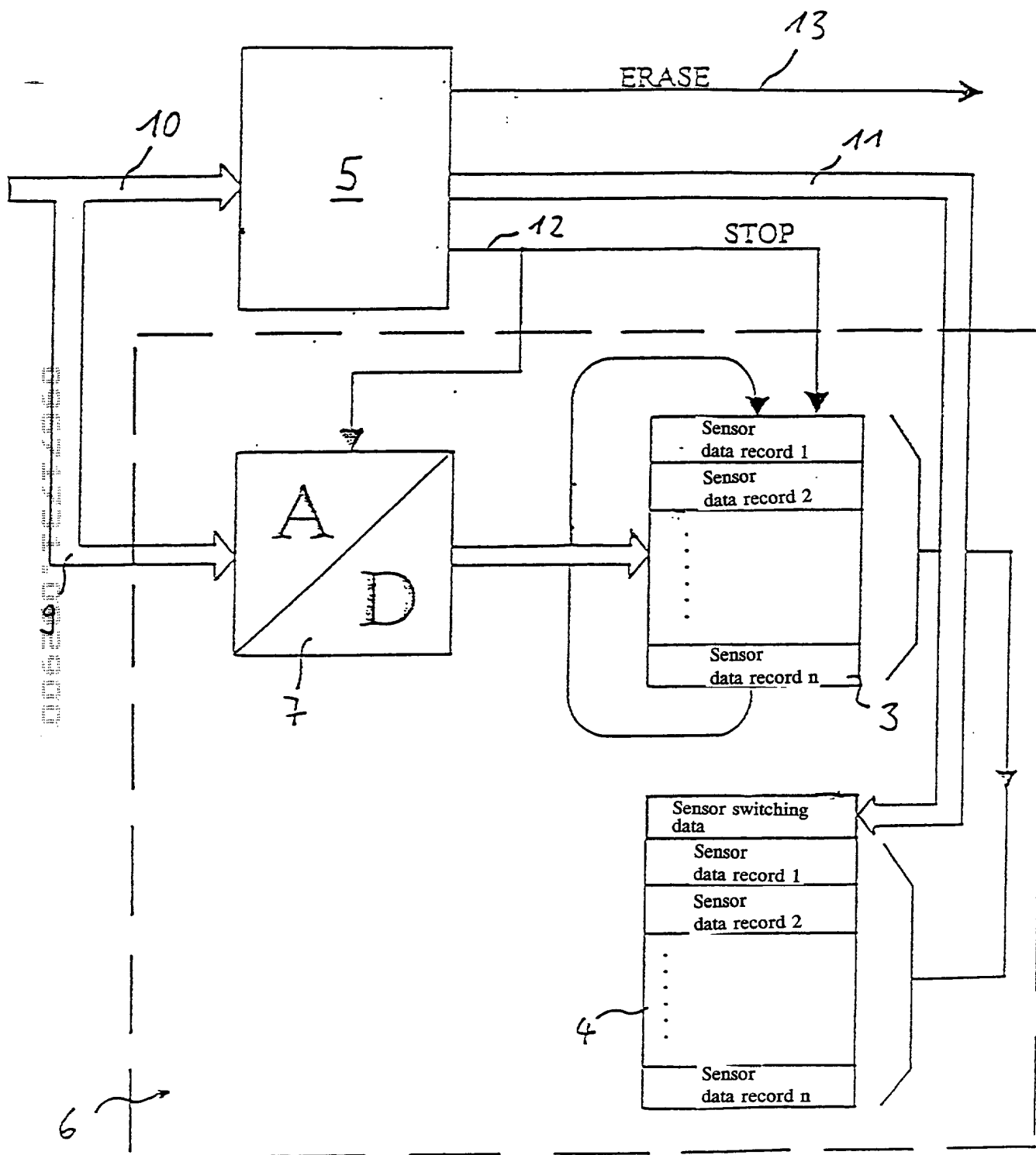


Fig 2

DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention (Design, if applicable) entitled: **METHOD FOR PROTECTING A DATA MEMORY**

the specification of which (check one):

☒ is attached hereto, or ☐ was filed on:

as U.S. Application Number or PCT International Application

Number:

and (if applicable) was amended on:

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56*. I hereby claim foreign priority benefits under *Title 35, United States Code §119* of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR FOREIGN APPLICATION(S)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No
199 47 574.1	Germany	01 October 1999	X	

☐ Additional Priority Application(s) Listed on Following Page(s)

I HEREBY CLAIM THE BENEFIT UNDER TITLE 35 U.S. CODE §119(E) OF ANY U.S. PROVISIONAL APPLICATIONS LISTED BELOW.	
Application Number	Day/Month/Year Filed

☐ Additional Provisional Application(s) Listed on Following Page(s)

I hereby claim the benefit under *Title 35, United States Code, §120* of any United States application(s) or PCT international application(s) designating The United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of *Title 35, United States Code, §112*, I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56* which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Number	Filing Date	Status - Patented, Pending or Abandoned

☐ Additional US/PCT Priority Application(s) listed on Following Page(s)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under *section 1001 of title 18 of the United States Code* and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: I (We) hereby appoint as my (our) attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: J. Ernest Kenney, Reg. No. 19,179; Eugene Mar, Reg. No. 25,893; Richard E. Fichter, Reg. No. 26,382; Thomas J. Moore, Reg. No. 28,974; Joseph DeBenedictis, Reg. No. 28,502; Benjamin E. Urcia, Reg. No. 33,805; and

I(we) authorize my(our) attorneys to accept and follow instructions from **Klunker Schmitt-Nilson Hirsch** regarding any matter related to the preparation, examination, grant and maintenance of this application, any continuation, continuation-in-part or divisional based thereon, and any patent resulting therefrom, until I(we) or my(our) assigns withdraw this authorization in writing.

Send correspondence to: **BACON & THOMAS, PLLC**
625 Slaters Lane - 4th Floor
Alexandria, VA 22314-1176

Telephone Calls to: **J. Ernest Kenney (703) 683-0500**

FULL NAME OF FIRST OR SOLE INVENTOR Dr. Thomas GRASSL	CITIZENSHIP German
RESIDENCE ADDRESS Ganzenmullerstrasse 6, D-85354 Freising, Germany	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

☒ See following page(s) for additional joint inventors.

CONTINUATION OF DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

Page 2

PRIOR FOREIGN APPLICATION(S) (35 USC §119)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No

PRIOR PROVISIONAL APPLICATIONS 35 U.S. CODE §119(E)	
Application Number	Day/Month/Year Filed

PRIOR U.S. OR PCT INTERNATIONAL APPLICATIONS (35 U.S. CODE §120)		
Application Number	Filing Date	Status - Patented, Pending or Abandoned

FULL NAME OF JOINT INVENTOR Arvid WIREN	CITIZENSHIP German
RESIDENCE ADDRESS Cosimastrasse 140, D-81927 Munchen, Germany	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

FULL NAME OF JOINT INVENTOR Walter STRAUB	CITIZENSHIP United States of America
RESIDENCE ADDRESS Buchlweg 42, D-82041 Oberhaching, Germany	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
RESIDENCE ADDRESS	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
RESIDENCE ADDRESS	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

☐ See following pages for additional joint inventors/priority applications.